Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently amended) A cryptography method, comprising:

determining information M to be encrypted; and

encrypting said information to form encrypted information using a non-trivial ci-quasigroup as a key K to create a cypher C indicative of the information M as C = M*K, where * denotes a mathematical operation, where the non-trivial ci-quasigroup has properties that for the operation *, between any two elements in the ~~group~~ non-trivial quasigroup, the result of the operation is also in the ~~group~~ non-trivial quasigroup and for every K, as M takes on a different value, the resulting values of C are each distinct, for every M, as K takes on all key values, the resulting values of C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$.

2. (Canceled)

3. (Previously presented) A method as in claim 1, further comprising decoding said information using the crossed-inverse function of said ci-quasigroup.

4. (Previously presented) A method as in claim 1, wherein said encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using said first result, and said encryption can be iterated an arbitrary number of times.

5. (Previously presented) A method as in claim 1 further comprising defining a rule indicative of said quasigroup.

6. (Original) A method as in claim 3 further comprising defining a rule indicative of said crossed inverse of said quasigroup.

7. (Original) A method as in claim 1 further comprising carrying out a second encrypting using said arithmetic, and wherein a result of said second arithmetic is encrypted exponentially more than a result of said first arithmetic.

8. (Previously presented) A method as in claim 1 wherein said encrypting comprises using a non trivial non-group crossed inverse quasigroup to encode.

9. (Original) A method as in claim 3 further comprising distributing information indicative of said quasigroup as a public key, and keeping secret the crossed inverse quasigroup.

10. (Previously presented) A method as in claim 1 wherein said quasigroup is formed by an n by n square, where n is greater than 10^{10}.

11. (Original) A method as in claim 4 wherein said first and second encryption form iterative encipherment.

12. (Original) A method as in claim 4 wherein said first interiation is carried out in a different direction than said first encryption.

13. (Original) A method as in claim 12 wherein said first direction is left to right and said second direction is right to left.

14. (Original) A method as in claim 1 wherein said encrypting is carried out using block ciphers.

15. (Original) A method as in claim 14 wherein said block cipher are defined by a function.

16. (Original) A method as in claim 14 wherein said block ciphers are formed using cross inversed quasigroups, used according to $C = f(M,K)$ for the encryption and $M=finv(C,K)$ for the decryption.

17-18. (Canceled)

19. (Currently amended) A cryptography method, comprising:

determining information to be encrypted; and

encrypting said information M to form encrypted information using a Key K which is a crossed-inverse quasigroup to create a cipher C as C = M*K, where * denotes a mathematical operation, where the quasigroup has properties that for the operation *, between any two elements in the ~~group~~ quasigroup, the result of the operation is also in the ~~group~~ quasigroup, and for every K, as M takes on different values, the resulting values of the cipher C, are each distinct, for every M, as K takes on all key values, the resulting values of the cipher C, are all distinct; and that each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$.

20. (Canceled)

21. (Original) A method as in claim 19, further comprising decoding using a crossed inverse of said quasigroup.

22. (Original) A method as in claim 1, wherein said encrypting comprises carrying out a first encryption to get a first result, then carrying out a second encryption using said first result.

23. (Original) A cryptography method comprising encrypting information using an arithmetic with an algebraic structure, said algebraic structure being a nongroup, nonfield structure.

24. (Original) A method as in claim 23 wherein said algebraic structure is not associative.

25. (Original) A method as claim 23 wherein said algebraic structure is not commutative.

26. (Original) A method as in claim 24 wherein said algebraic structure is not commutative.

27-28. (Canceled)

29. (Previously Presented) An apparatus comprising a program stored on a computer readable media including instructions to:

encrypt a message M into an encrypted message using a key K indicative of a crossed-inverse quasigroup representation, where the quasigroup has properties that for an operation *, between any two elements in the ~~group~~ quasigroup, ~~the~~ a result of the operation is also in the ~~group~~ quasigroup, and for every K, as M takes on message values, ~~the~~ resulting values of a cipher C, where C = M*K are each distinct, for every M, as K takes on all key values, ~~the~~ resulting values of the cipher C, are all distinct; and each key K in a keyspace P has a permutation K^{-1} that decodes the encrypting, such that $K^{-1}*(M*a) = M$;

send the encrypted message C; and

decrypt the encrypted message using information indicative of the same crossed-inverse quasigroup representation.

30. (Canceled)

31. (Original) An apparatus as in claim 29, wherein said arithmetic is one which is based on a multiplication table which is expressed as a rule.

32. (Original) An apparatus as in claim 29, further comprising adding a random seed to said arithmetic.

33. (Previously presented) An apparatus as in claim 29, further comprising using an additional encryption to provide an effective key size of x^2 of the original encryption.

34. (Canceled)

35. (New) A method as in claim 1, further comprising sending the encrypted information as a message.

36. (New) A method as in claim 19, further comprising sending the encrypted information as a message.